3GPP TSG SA WG3 Security — S3#21 **S3-010696**

27-30 November, 2001

Sophia Antipolis, France

From: **SA3**

To: **CN5**

Title: **Support of security algorithms in OSA framework**

Contact: **Peter Howard, Vodafone Group**
peter.howard@vodafone.com

SA3 would like to thank CN5 for its reply LS on the support of security algorithms in the OSA framework (S3-010661 = N5-011159).

SA3 thank CN5 for the clarifications on how the authenticate method of the IpClientAPILevelAuthentication interface is used.

SA3 have reviewed the draft CR to TS 29.198 which attempts to address SA3's previous comments. Unfortunately it appears that some of SA3's comments have not been fully addressed in the draft CR:

- The mode of operation of the algorithms is still missing. For example, for single DES, FIPS 46-3 only specifies the DES block cipher, not the mode of operation in which DES can be used to encrypt data. A mode of operation from FIPS 81 could be used, e.g. CBC.
- It is noted that a new TPEncryptionCapability called P_DES_112, is added for triple DES. It is acknowledged that the old P_DES_128 cannot be removed for backward compatibility reasons. However, SA3 would prefer that the description of P_DES_128 is changed to make it clear that this algorithm effectively uses a 112 bit key.
- If CN5 cannot remove 56 bit DES and 512 bit RSA for backwards compatibility reasons then it is requested that a note is added below the table to indicate that these algorithms might not be secure enough for this particular application. A similar note should also be added regarding the inclusion of MD5 which is contained in section 4.1.2 (TpSigningAlgorithm) of the specification.
- The inclusion of SHA1 and DSA as a type of encryption method is misleading. It was SA3's intention for CN5 to consider DSA as an additional Signing Algorithm and SHA-1 as a replacement for MD5 in the RSA signature methods in section 4.1.2 (TpSigningAlgorithm) of the specification.

SA3 also have the following additional comments:

- The inclusion of RSA authentication as a type of encryption method is misleading. Do CN5 really mean RSA encryption?

In answer to the question about the reference for RIPEMD, CN5 is informed that ISO/IEC 10118-3 (Dedicated hash functions) may be used.

Unfortunately due to time constraints at our meeting and lack of information/expertise on the OSA framework security mechanisms, SA3 were unable to produce a new proposal for a CR which addresses all of our concerns. Furthermore, as the current draft CR is only a partial solution, it is recommended not to submit it to CN for approval at this time. Instead it is recommended that the work to resolve these outstanding security issues is done within SA3 in collaboration with OSA experts from CN5 and the results communicated to CN5.